JCSCR
Journal of Computer Science & Research

Journal of Computer Science & Research (JCSCR) - ISSN 2227-328X
http://www.jcscr.com
Vol. 1, No. 4, Pages. 14-20, August 2012

WiMAX Security: Problems & Solutions

Paul Semaan

LACSC – Lebanese Association for Computational Sciences
Registered under No. 957, 2011, Beirut, Lebanon

Abstract

This paper is a survey discussing the WiMAX technology and its security features. The paper starts with the history of WiMAX, then it goes into reviewing its security features and properties such as data association and user authorization. Next, data encryption algorithms are to be examined including DES and AES. Finally, the various security threats and vulnerabilities that face WiMAX technology are to be discussed elaborately.

Keywords

WiMAX, Security, Encryption, Authentication

1. Introduction

WiMAX stands for worldwide interoperability for microwave access. It was proposed to facilitate high-speed data distribution through wireless metropolitan area networks (WMANs) [1]. With the advantages of rapid deployment, high scalability, and low upgrade cost, WiMAX attempts to tackle the last mile bottleneck problem of current telecommunications networks.

The IEEE 802.16 working group on broadband wireless access (BWA) standards develops standards and recommends practices to support the development and deployment of the WiMAX technology.

2. History and Different Releases

The first WiMAX standard, IEEE 802.16-2001, was published in 2002. It defines a point-to-multipoint (PMP) fixed wireless access system between a base station (BS) and its associated subscriber stations (SSs). It operates in the 10–66 GHz frequency range, which is the so-called line-of-sight (LOS) communications.

The IEEE 802.16-2004 standard was published in 2004 to extend the WiMAX specification into the 2–11GHz frequency range, the so-called nonline-of-sight (NLOS) operation. It also describes the WiMAX system profiles and conformance criteria to adapt to the dynamic wireless environment. By introducing the mesh mode, IEEE 802.16-2004 is capable of forwarding traffic from a node to its neighboring nodes.

The latest WiMAX standard, IEEE 802.16e-2005, was approved in December 2005. By employing scalable orthogonal frequency division multiplexing (SOFDM), IEEE 802.16e-2005 provides full mobility support for both licensed and unlicensed spectra.

3. Security Features

WiMAX security has two goals, one is to provide privacy across the wireless network and the other is to provide access control to the network [2].

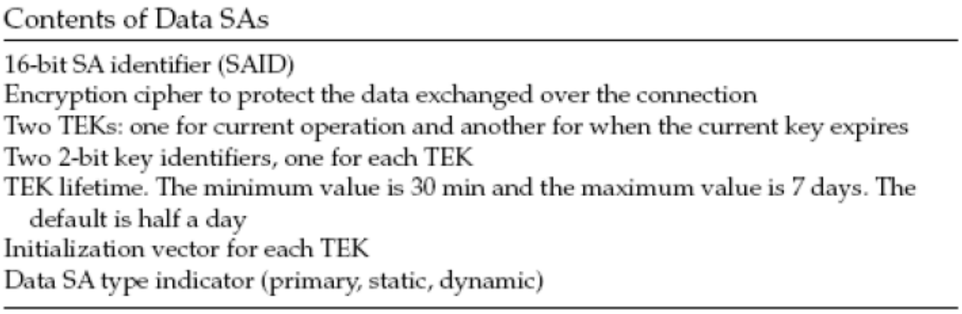
Privacy is accomplished by encrypting connections between the subscriber station and the base station. The base station protects against unauthorized access by enforcing encryption of service flows across the network. A privacy and key management (PKM) protocol is used by the base station to control the distribution of keying data to subscriber stations. This allows the subscriber and base stations to synchronize keying data. Digital-certificate-based subscriber station authentication is included in the PKM to provide access control [3].

3.1. Security Associations

A security association (SA) is the set of security information a base station and one or more of its client subscriber stations share to support secure communication across a WiMAX network. WiMAX uses two different types of SAs, data and authorization [3, 4].

3.1.1. Data Security Associations

There are three different types of data SAs: primary, static, and dynamic. Primary SAs are established by the subscriber stations during their initialization process. The base station provides the static SAs. Dynamic SAs are established and eliminated as needed for service flows. Both static and dynamic SAs can be shared among multiple subscriber stations [5]. Figure 1 shows the content of a data SA.



Contents of Data SAs

16-bit SA identifier (SAID)
Encryption cipher to protect the data exchanged over the connection
Two TEKs: one for current operation and another for when the current key expires
Two 2-bit key identifiers, one for each TEK
TEK lifetime. The minimum value is 30 min and the maximum value is 7 days. The default is half a day
Initialization vector for each TEK
Data SA type indicator (primary, static, dynamic)

Figure 1 - Authorization SA

The *SA identifier* (*SAID*) is used to uniquely identify the data SA.

The *encryption cipher* defines what method of encryption will be used to encrypt data. Initially, the IEEE 802.16 standard defined the use of the data encryption standard (DES) in cipher block chaining (CBC) mode.

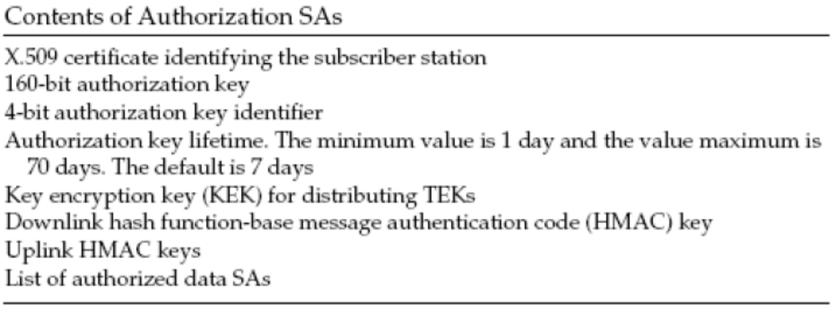
Traffic encryption keys (*TEKs*) are used to encrypt data transmissions between the base stations and subscriber stations. The data SA defines two TEKs, one for current operations and a second to be used when the current one expires. Two TEK identifiers are included, one for each key. A TEK lifetime is also included to indicate when the TEK expires. The default lifetime is half a day, but it can vary from 30 min to 7 days.

DES in CBC mode requires an *initialization vector* to operate. Therefore, one for each TEK is included in the data SA. Both initialization vectors are 64 bits in length to accommodate the 64-bit block size used in DES encryption.

The *data SA type* is also included to indicate whether it is a primary, static, or dynamic data SA.

3.1.2. Authorization Security Associations

Authorization SAs are shared between a base station and a subscriber station. They are used by the base station to configure data SAs for the subscriber station [4]. Figure 2 shows the contents of an authorization SA.



Contents of Authorization SAs

X.509 certificate identifying the subscriber station
160-bit authorization key
4-bit authorization key identifier
Authorization key lifetime. The minimum value is 1 day and the value maximum is 70 days. The default is 7 days
Key encryption key (KEK) for distributing TEKs
Downlink hash function-base message authentication code (HMAC) key
Uplink HMAC keys
List of authorized data SAs

Figure 2 - Authorization SA

An *X.509 certificate* is included, which allows the base station to identify the subscriber station.

The *160-bit authorization key* (*AK*) is included to allow the base station and subscriber station to authenticate each other during TEK exchanges.

A 4-bit *AK identifier* is used to distinguish among different AKs.

An *AK lifetime* is also included to indicate when the AK expires. The default lifetime is 7 days, but it can range from 1 to 70 days.

Key encryption keys (*KEKs*) are used to encrypt TEKs during the TEK exchange process. Two KEKs are required for the encryption process and are derived from the AK. The KEKs are computed by first concatenating the hex value 0x53 repeated 64 times and the AK. Then the SHA-1 hash of this value is computed, which outputs 160 bits. Finally, the first 128 bits of the output are taken and divided into two 64-bit TEKs. These two TEKs are included in the authorization SA.

JCSCR
Journal of Computer Science & Research

Journal of Computer Science & Research (JCSCR) - ISSN 2227-328X
http://www.jcscr.com
Vol. 1, No. 4, Pages. 14-20, August 2012

Two *hashed message authentication code* (*HMAC*) keys, one for uplink and one for downlink, are included to allow for the creation of HMACs during the TEK exchange process. The uplink key is used to create an HMAC of messages to be sent, while the downlink key is used to create an HMAC of messages received, allowing the receiver to authenticate the message. The uplink key is obtained by concatenating the hex value 0x3A repeated 64 times and the AK, then computing the SHA-1 hash of this value, creating a 160-bit HMAC key. The downlink key is computed in the same fashion, but the hex value 0x5C is concatenated with the AK instead.

A *list of authorized data SAs* is also included in the authorization SA that provides the subscriber station with the knowledge of the data SAs it can request.

3.2. Authentication

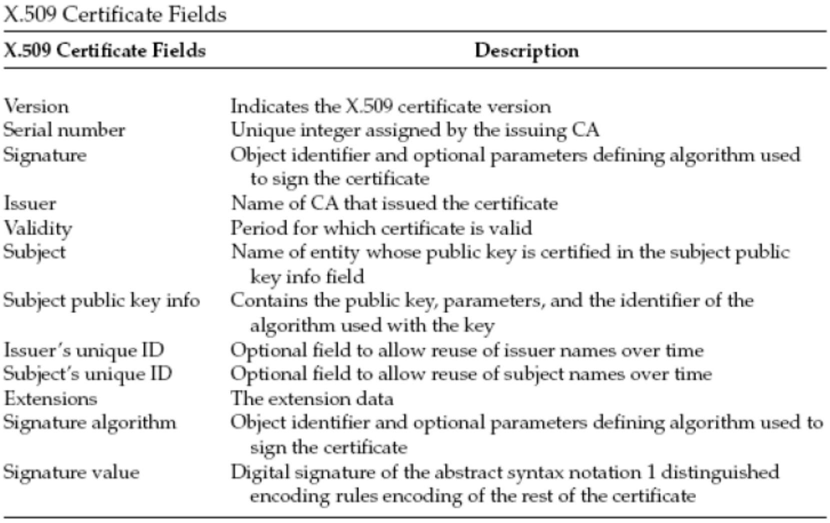
3.2.1. Hashed Message Authentication Code

HMACs are used to provide message authentication. By using HMACs, the receiver can verify who sent the message. This is possible because the sender creates an HMAC of the message it wishes to send using a key known only by the sender and receiver. When the receiver gets the message, it computes its own HMAC of the message using the same key and compares the one it computed with the one received from the sender. If the HMACs match then the sender is confirmed.

3.2.2. X.509 Certificates

X.509 certificates are used to allow the base station to identify subscriber stations. Table 11.6 describes the required fields as defined by the IEEE 802.16 standard. While extension data may be included, the standard does not define any [3,4].

There are two types of certificates: *manufacturer certificates* and *subscriber station certificates*. A manufacturer certificate, which identifies the manufacturer of the device, can be a self-signed certificate or issued by a third party. A subscriber station certificate is typically created and signed by the manufacturer of the station. It is used to identify a subscriber station and includes the MAC address of the station in the subject field. Base stations can use the manufacturer certificate to verify the subscriber station's certificate, allowing it to determine if the device is legitimate [4]. Figure 3 depicts the structure on a X.509 certificate.



X.509 Certificate Fields

X.509 Certificate Fields	Description
Version	Indicates the X.509 certificate version
Serial number	Unique integer assigned by the issuing CA
Signature	Object identifier and optional parameters defining algorithm used to sign the certificate
Issuer	Name of CA that issued the certificate
Validity	Period for which certificate is valid
Subject	Name of entity whose public key is certified in the subject public key info field
Subject public key info	Contains the public key, parameters, and the identifier of the algorithm used with the key
Issuer's unique ID	Optional field to allow reuse of issuer names over time
Subject's unique ID	Optional field to allow reuse of subject names over time
Extensions	The extension data
Signature algorithm	Object identifier and optional parameters defining algorithm used to sign the certificate
Signature value	Digital signature of the abstract syntax notation 1 distinguished encoding rules encoding of the rest of the certificate

Figure 3 - X.509 Certificate

3.3 Privacy and Key Management

Subscriber stations use the PKM protocol to obtain authorization and traffic keying material from the base station. The PKM protocol can be broken into two parts. The first handles subscriber station authorization and AK exchange. The second handles TEK exchange [5].

3.3.1. Authorization and AK Exchange

PKM authorization is used to exchange an AK from the base station to the subscriber station. Once the subscriber station receives an initial authorization, it will periodically seek reauthorization. The AK exchange is accomplished using three messages, and is illustrated in Figure 4.

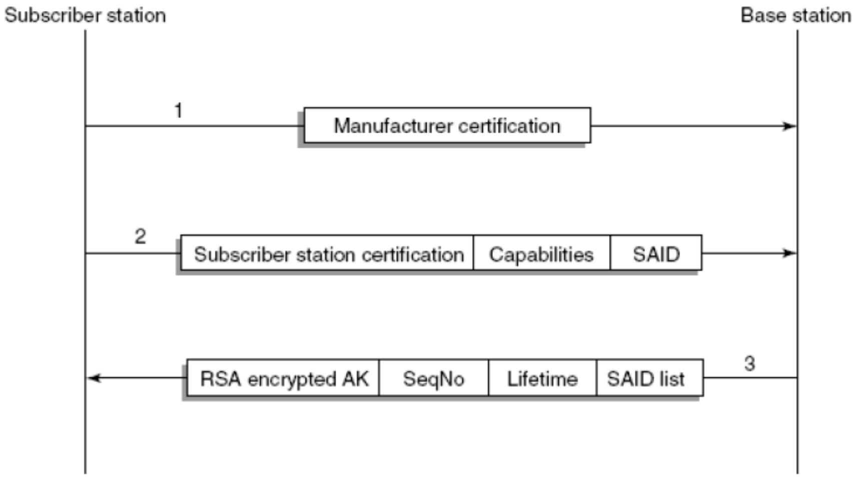


Figure 4 - AK Exchange

The subscriber station initiates the exchange by sending a message containing the subscriber station manufacturer's X.509 certificate to the base station. The message is strictly informative and can be ignored by the base station. However, base stations can be configured to only allow access to devices from trusted manufacturers.

The second message is sent from the subscriber station to the base station immediately after the first message. This message is a request for an AK and a list of SAIDs that identify SAs the subscriber station is authorized to participate in. There are three parts to the message: a manufacturer-issued X.509 certificate, cryptographic algorithms supported by the subscriber station, and the SAID of its primary SA.

The base station uses the subscriber station's certification to determine if it is authorized. If it is, the base station will respond with the third message. The base station uses the subscriber station's public key, obtained from its certification, to encrypt the AK using RSA. The encrypted AK is then included in the message along with the SeqNo, which distinguishes between successive AKs, the key lifetime, and a list of SAIDs of the static SAs the subscriber station is authorized to participate in.

3.3.2. TEK Exchange

Once the subscriber station has been authorized, it will establish an SA for each SAID in the list received from the base station. This is accomplished by initiating a TEK exchange. Once an SA is established, the subscriber station will periodically refresh keying material. The base station can also force re-keying if needed. Figure 5 illustrates the TEK exchange process.

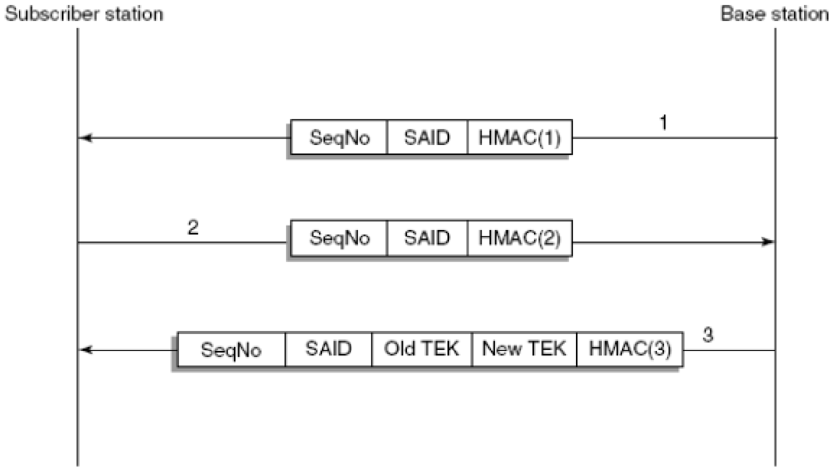


Figure 5 - TEK Exchange Process

The first message of a TEK exchange is optional and allows the base station to force re-keying. There are three parts to the message: SeqNo refers to the AK used in creating the HMAC, the SAID refers to the SA that is being re-keyed, and the HMAC allows the subscriber station to authenticate the message.

Journal of Computer Science & Research (JCSCR) - ISSN 2227-328X
http://www.jcscr.com
Vol. 1, No. 4, Pages. 14-20, August 2012

The second message is sent by the subscriber station in response to the first message or if the subscriber station wants to refresh the keying material. There are three parts to the message: SeqNo refers to the AK used in creating the HMAC, the SAID refers to either the SAID received in the first message or one of the SAs from the subscriber station's authorized SAID list, and the HMAC allows the base station to authenticate the message. If the HMAC in the second message is valid then the base station will send the third message. As in the first two messages, a SeqNo, the SAID, and the HMAC are included. In addition to these the old TEK and a new TEK are added. The old TEK just reiterates the active SA parameters while the new TEK is to be used when the active one expires. The base station encrypts both the old and new TEKs using triple DES in electronic code book (ECB) mode with the KEK associated with the SA.

Figure 6 illustrates the TEK encryption process. Here, KEK 1 is the leftmost 64 bits of the computed KEK and KEK 2 is the rightmost 64 bits. These two keys are used in the triple DES encryption in which the TEK is first encrypted using KEK 1. The output is then decrypted using KEK 2 and then encrypted using KEK 1. This process is performed on both the old and new TEKs to produce two encrypted TEKs.

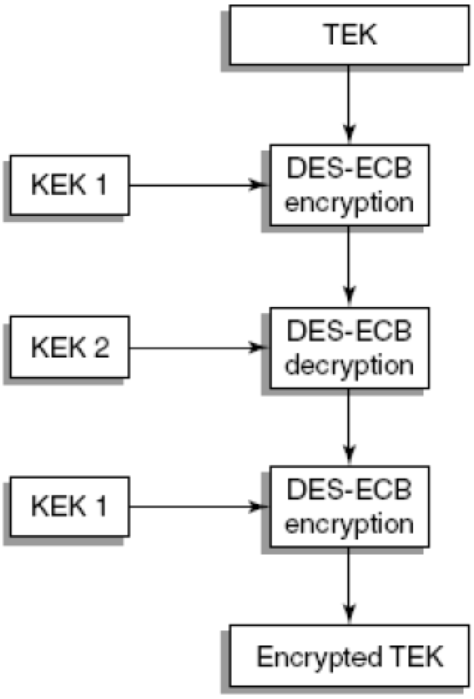


Figure 6 - Triple DES Encryption

3.3. Data Encryption

To provide privacy for the data being transmitted in WiMAX networks, the IEEE 802.16 standard employed the use of DES in CBC mode. Currently, DES is considered to be insecure and has been replaced by the AES. Therefore, the IEEE 802.16e standard defines the use of AES for use in encryption [4].

3.3.1. DES

Using DES in CBC mode, the payload field of the MAC PDU is encrypted, but the GMH and CRC are not. Figure 7 illustrates the encryption process.

Journal of Computer Science & Research (JCSCR) - ISSN 2227-328X
http://www.jcscr.com
Vol. 1, No. 4, Pages. 14-20, August 2012

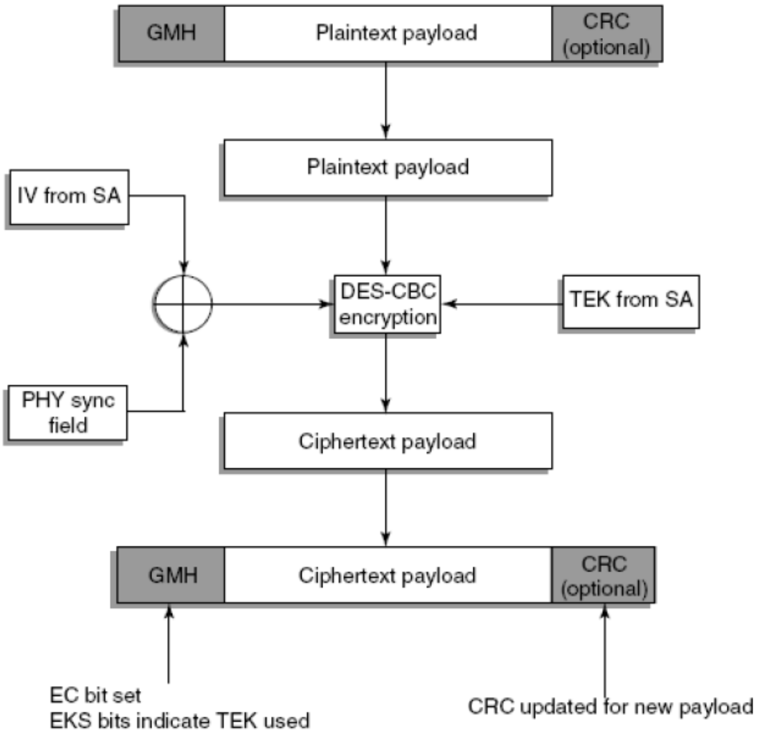


Figure 7 - WiMAX Encryption Process

CBC mode requires an initialization vector (IV), which is computed by taking the XOR of the IV parameter in the SA and the content of the PHY synchronization field. The DES encryption process uses the IV and the TEK from the SA of the connection to encrypt the payload of the PDU. This ciphertext payload then replaces the original plaintext payload. The EC bit in the GMH will be set to 1 to indicate an encrypted payload and the EKS bits will be set to indicate that the TEK was used to encrypt the payload. If the CRC is included, it will be updated for the new ciphertext payload [5].

3.3.2. AES

The IEEE 802.16e standard added the use of AES to provide stronger encryption of data. It defines the use of AES in four modes: CBC, counter encryption (CTR), CTR with CBC message authentication code (CCM), and ECB. CTR mode is considered better than CBC mode due to its ability to perform parallel processing of data, preprocessing of encryption blocks, and is simpler to implement. CCM mode adds the ability to determine the authenticity of an encrypted message to CTR mode. ECB mode is used to encrypt TEKs.

4. Security Threats

In WiMAX, security threats apply to both the PHY and MAC layers. Possible PHY level attacks include jamming of a radio spectrum, causing denial of service to all stations, and flooding a station with frames to drain its battery. Currently, there are no efficient techniques available to prevent PHY layer attacks. Therefore, the focus of WiMAX security is completely at the MAC level [4]. In this section, we discuss some of the open security issues in the WiMAX networks.

5.1. Authorization Vulnerabilities

A major vulnerability of WiMAX security is the lack of a base station certificate, which is needed for mutual authentication. Without mutual authentication, the subscriber stations cannot verify that authorization protocol messages received are from the base station. This leaves the subscriber station open to forgery attacks, allowing any rogue base station to send it responses [4].

A solution to issues with WiMAX's authentication and authorization proposes the wireless key management infrastructure (WKMI), which is based on the IEEE 802.11i standard. WKMI is a key management hierarchy infrastructure that is based on the use of X.509 certificates allowing subscriber stations and base stations to perform mutual authentication and key negotiation. AK generation is another concern with the authorization protocol. Though the standard assumes a random AK generation, it imposes no requirements.

An additional weakness lies in the fact that the base stations generate the AK, requiring the subscriber station to trust that the base station always generates a new AK that is cryptographically separated from all other AKs previously generated. To hold true, the base stations must have a perfect random number generator. Allowing both the subscriber station and base station to contribute to the AK generation could solve this issue [4].

5.2. Key Management

A major issue with key management in WiMAX is the size of its TEK identifier. Currently, a 2-bit number is used, which allows only four values (0 to 3) to be represented. This causes the TEK identifier to wrap from3 to 0 on every fourth key, leaving stations open to replay attacks in which an attacker could reuse expired keys. To solve this issue, the TEK identifier's size needs to be increased to prevent wrapping. If the longest AK lifetime (70 days) and the shortest TEK lifetime (30 min) are considered, then 3360 different TEKs need to be represented, which would require 12 bits be used for the TEK identifier [4].

Another issue is the TEK lifetime, which can be set anywhere between 30 min and 7 days with a default of half a day. If DES in CBC mode is used for encryption with the possible lifetime values, the security of the data may be compromised. This is due to the fact that DES in CBC mode becomes insecure after operating on 2n/2 blocks with the same encryption key, where n is the block size. Since DES uses a 64-bit block size, after 232 blocks the encryption will be insecure. The time it takes to happen depends on the average throughput between stations. Considering the high transfer rates WiMAX offers and the ability to choose a larger TEK lifetime, encryption insecurity is highly possible. The introduction of AES in the IEEE 802.16e standard will help solve the TEK lifetime issues. Unfortunately, implementation of this standard is still a way off, possibly leaving current deployments of WiMAX insecure.

Acknowledgment

This research was funded by the Lebanese Association for Computational Sciences (LACSC), Beirut, Lebanon, registered under Decree No. 957, 2011, Beirut, Lebanon.

References

[1] Z. Abichar, P. Yanlin, and J.M. Chang, "WiMAX: The emergence of wireless Broadband", IT Professional, vol. 8, pp. 44–48, 2006.

[2] B. Rathgeb and C. Qiang, "Utilizing the IEEE 802.16 Standard for Homeland Security Applications", Orlando, FL, 2005.

[3] IEEE standard for local and metropolitan area networks -Part 16: Air interface form fixed broadband wireless access systems, IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001), pp. 851–857, 2004.

[4] D. Johnston and J. Walker, "Overview of IEEE 802.16 security", IEEE Security & Privacy", vol. 2, pp. 40–48, 2004.

[5] IEEE standard for local and metropolitan area networks. Part 16: air interface for fixed and mobile broadband wireless access systems amendment 2: Physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum, Based on IEEE Standard 802.16, Wuhan, China, 2005.

[6] Airspan, "Mobile WiMAX security," Airspan Networks Inc. 2007, http://www.airspan.com.